**Lab 7: Creating VLAN and VLAN Trunking using Packet Tracer**

**Theory**

A VLAN (Virtual Local Area Network) segments a single physical network into multiple logical networks. Each VLAN operates as an independent network, even though they share the same physical infrastructure. VLANs enhance network security, reduce broadcast traffic, and allow administrators to logically segment traffic based on factors like department or function within an organization. This segmentation improves overall network efficiency and management.

**VLAN Trunking**

VLAN trunking allows traffic from multiple VLANs to travel over a single network link between switches or other network devices. This is done by tagging Ethernet frames with a VLAN identifier, typically using IEEE 802.1Q tagging. Trunking extends VLANs across network devices, providing greater flexibility in network design and enabling VLANs to span different physical locations.

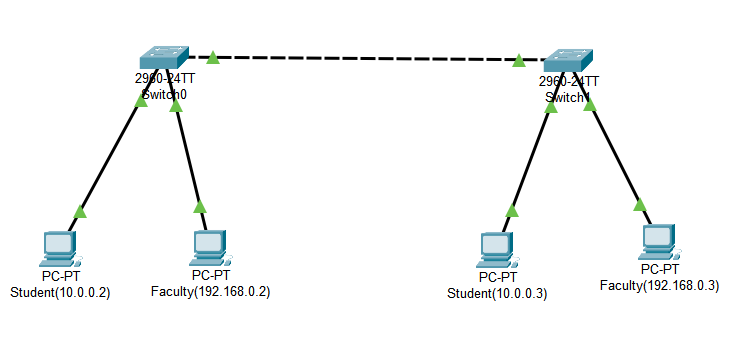
**VLAN Architecture**

VLAN architecture logically groups devices across different network segments, creating multiple broadcast domains on a single infrastructure. Each VLAN acts as a separate network, isolating traffic unless allowed through routing or firewall rules. Key components include access ports (connecting devices to VLANs), trunk ports (carrying traffic for multiple VLANs), and VLAN-aware devices. This design enhances scalability, security, and performance

**Component Used**

**Hardware:** Switches (2), Ethernet cables, End devices(4).

**Software:** Cisco Packet Tracer

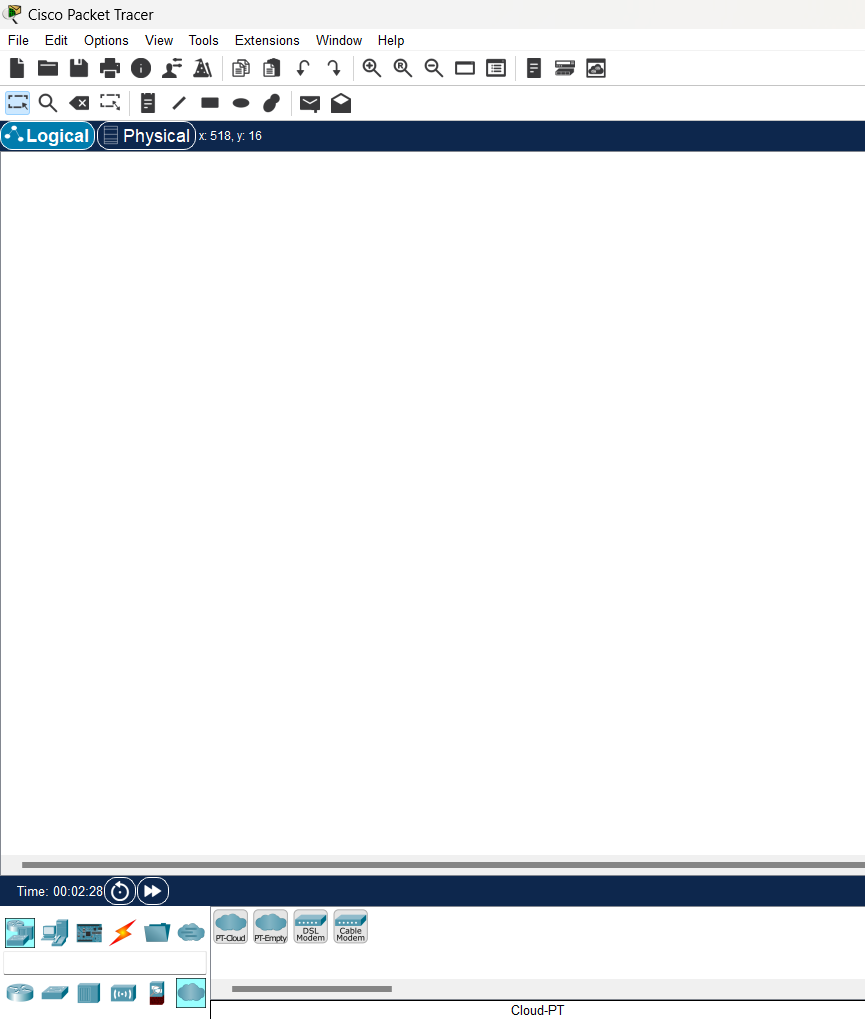
**Network Diagram**

*Fig: Network map for VLAN*

**Procedure**

Here is the procedure for creating the LAN network shown in the image using Cisco Packet Tracer:

**Step 1: Launch Cisco Packet Tracer**

*Fig: Workspace for network design*

**Step 2: Add the network devices to the workspace and connecting devices:**

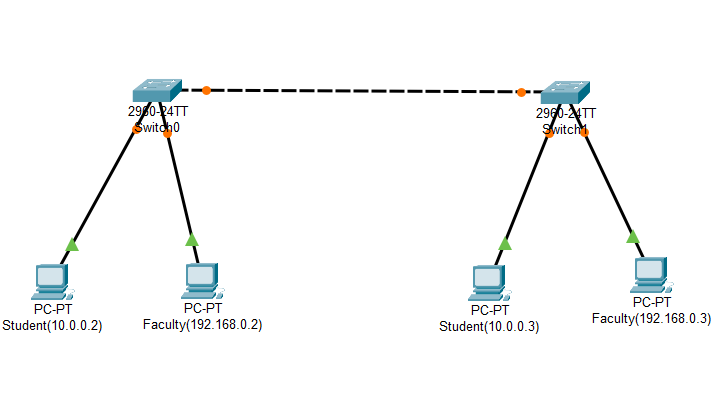
2.1 From the Device-Type Selection box, choose the following devices and add them to the workspace:

2.2 One 2960-24TT Switch and four PC’s

2.3 Use the copper straight-through cable to connect each PC to one of the available ports on the switch.

2.4 Ensure that each connection is made properly.

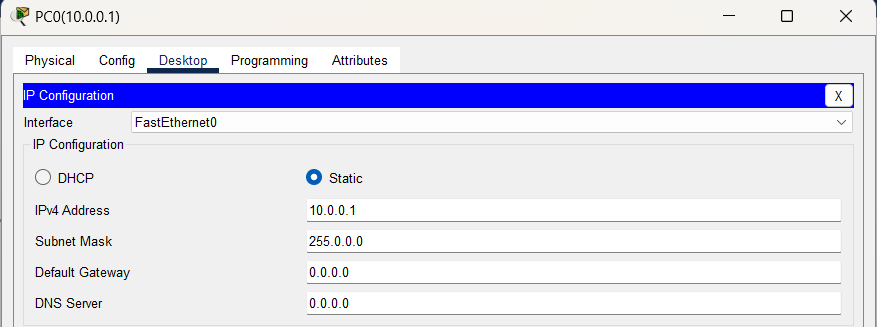
2.5 Also renamed the PC’s as student(10.0.0.2), Faculty(192.168.0.2), student(10.0.0.3), and Faculty(192.168.0.3).

*Fig:Connection between all devices in VLAN*

**Step 4: Configure IP addresses:**

4.1 Right-click on each PC and select "IP Configuration."

4.2 In the IP Configuration window, assign IP addresses as follows: Student devices - 10.0.0.2 and 10.0.0.3; Faculty devices - 192.168.0.2 and 192.168.0.3. Student devices will connect via port Fa 0/1, while Faculty devices will connect via port Fa 0/2.

*Fig:IP configuration*

**Step 5: Configuring VLANs :**

**5.1 Create VLAN on Both Switches & Assign Port to Both Switches:**  
To create VLANs on both switches, enter configuration mode and use the vlan <VLAN\_ID>` command to define separate VLANs for Student and Faculty devices. After creating the VLANs, assign ports by selecting the specific interfaces (e.g., Fa 0/1 for Students and Fa 0/2 for Faculty). Use the `switchport mode access` command to set the interface mode and then the `switchport access vlan <VLAN\_ID>` command to associate the ports with the appropriate VLAN. Repeat the process on both switches for all necessary ports.

**5.2 Create Trunking on Both Switches:**  
 To enable trunking, configure the interfaces between the two switches using the switchport mode trunk command. This allows multiple VLANs to pass through the same link, facilitating communication between devices in the same VLAN but connected to different switches. Trunking ensures that tagged traffic is carried across the switches while maintaining VLAN distinctions.

**Code for VLAN configurations:**

Switch(config)#vlan 10

Switch(config-vlan)#name student

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name faculty

Switch(config-vlan)#exit

Switch(config)#exit

**Code for Assigning ports:**

Switch#config t

Switch(config)#int fa 0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#int fa 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Switch(config-if)#exit

Switch(config)#exit

**Code for Trunking Switches:**

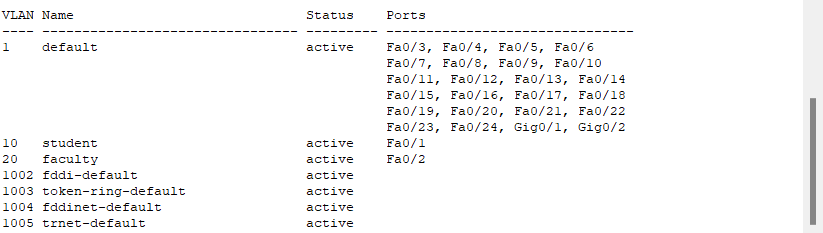
Switch#config t

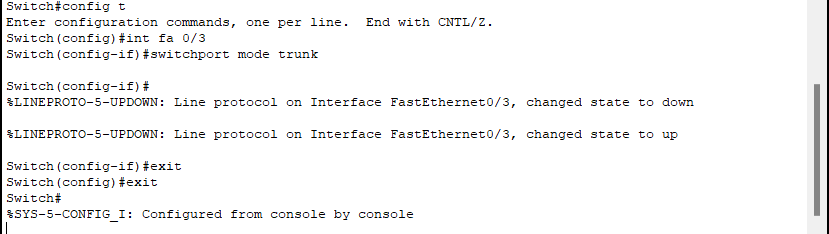
Switch(config)#int fa 0/3

Switch(config-if)#switchport mode trunk

Switch(config-if)#exit

Switch(config)#exit

*******Fig:Assigning ports to VLAN*

**

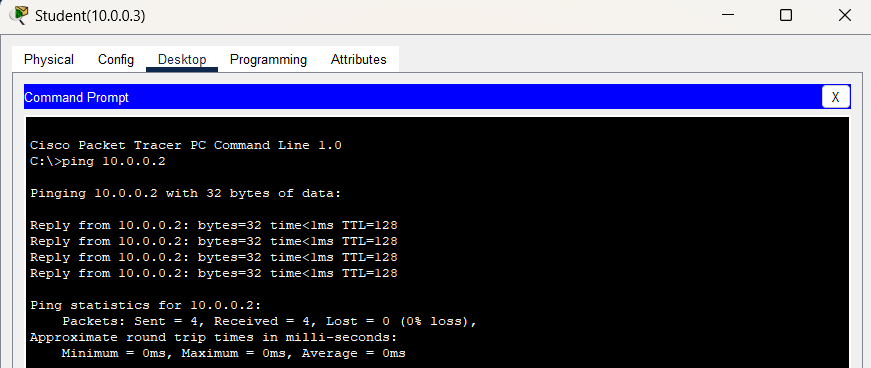
*Fig:Configuring trunking between switches*

**Step 7: Verify connectivity**

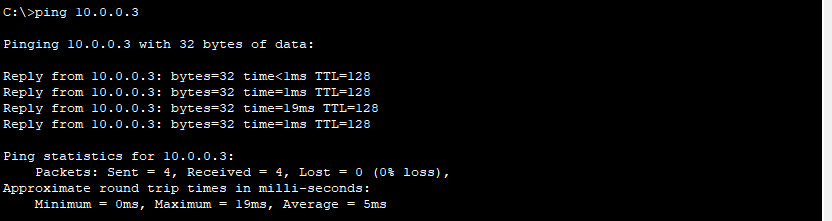
7.1 To test whether the network is working, you can ping other devices on the network from each PC.

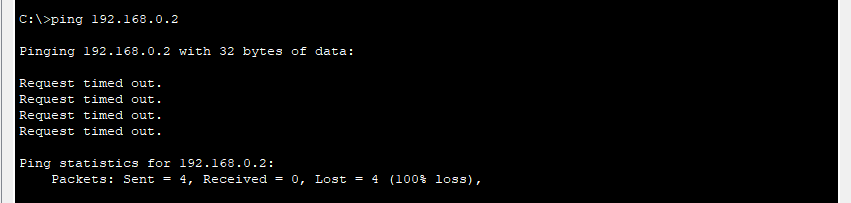
7.2 Now ping student(10.0.0.2) from student(10.0.0.3) and vice-versa.

7.3 Also ping student(10.0.0.2) from faculty(198.68.0.2) to check there is no connection between student and faculty.

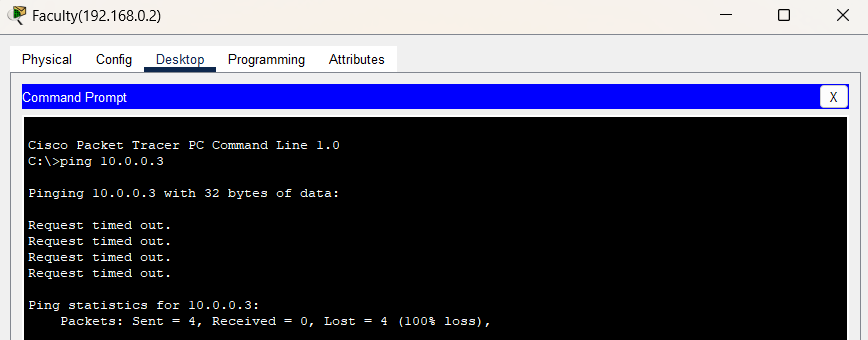
7.4 If the ping is successful, you should see replies from the other device.

*Fig:Connectivity test from student(10.0.0.3) to student (10.0.0.2)*

**

*Fig:Connectivity test from student(10.0.0.2) to student (10.0.0.3)*

*Fig:Connectivity test from student(10.0.0.2) to faculty(192.168.0.2)*

*Fig:Connectivity test from faculty(192.168.0.2) to student(10.0.0.3)*

**Conclusion**

In conclusion, creating VLANs and implementing VLAN trunking using Cisco Packet Tracer significantly enhances network segmentation and management. By assigning devices to distinct VLANs, you effectively reduce broadcast domains, improve security, and optimize network performance. VLAN trunking, which allows multiple VLANs to be transmitted across a single link, ensures efficient communication between VLANs across switches. This approach underscores the importance of structured network design in minimizing broadcast traffic and simplifying network administration, ultimately contributing to the scalability and efficiency of modern networks.